Sécurité Réseaux

AbdelAli Saidi
abdelali.saidi@gmail.com

2012/2013

Plan

Plan

Classification des attaques réseaux

Classification des attaques réseaux

- Attaques structurées ou d'expert

Classification des attaques réseaux

- Attaques structurées ou d'expert
- Attaques non structurées ou de novices

Classification des attaques réseaux

- Attaques structurées ou d'expert
- Attaques non structurées ou de novices
- Attaques externes

Classification des attaques réseaux

- Attaques structurées ou d'expert
- Attaques non structurées ou de novices
- Attaques externes
- Attaques internes

Classification des attaques réseaux

- Attaques structurées ou d'expert
- Attaques non structurées ou de novices
- Attaques externes
- Attaques internes
- Attaques directes

Classification des attaques réseaux

- Attaques structurées ou d'expert
- Attaques non structurées ou de novices
- Attaques externes
- Attaques internes
- Attaques directes
- Attaques par rebond

Plan

Phases d'une attaque typique

Phases d'une attaque typique

- Définition du but de l'attaque

Phases d'une attaque typique

- Définition du but de l'attaque
- Reconnaissance avant l'attaque

Phases d'une attaque typique

- Définition du but de l'attaque
- Reconnaissance avant l'attaque
- Choix et lancement de l'attaque

Phases d'une attaque typique

- Définition du but de l'attaque
- Reconnaissance avant l'attaque
- Choix et lancement de l'attaque
- Après l'attaque?

Phases d'une attaque typique

Définition du but de l'attaque

L'établissement visé

Pour une attaque structuré, l'établissement visé est choisi bien auparavant. Par exemple:

Objectifs

Phases d'une attaque typique

Définition du but de l'attaque

L'établissement visé

Pour une attaque structuré, l'établissement visé est choisi bien auparavant. Par exemple:

- Un concurrent

Objectifs

Phases d'une attaque typique

Définition du but de l'attaque

L'établissement visé

Pour une attaque structuré, l'établissement visé est choisi bien auparavant. Par exemple:

- Un concurrent
- Un "convive" (au réseau LAN)

Objectifs

Phases d'une attaque typique

Définition du but de l'attaque

L'établissement visé

Pour une attaque structuré, l'établissement visé est choisi bien auparavant. Par exemple:

- Un concurrent
- Un "convive" (au réseau LAN)
- L'ex-société

Objectifs

Phases d'une attaque typique

Définition du but de l'attaque

L'établissement visé

Pour une attaque structuré, l'établissement visé est choisi bien auparavant. Par exemple:

- Un concurrent
- Un "convive" (au réseau LAN)
- L'ex-société
- Un site e-commercial

Objectifs

Phases d'une attaque typique

Définition du but de l'attaque

L'établissement visé

Pour une attaque structuré, l'établissement visé est choisi bien auparavant. Par exemple:

- Un concurrent
- Un “convive” (au réseau LAN)
- L'ex-société
- Un site e-commercial

Objectifs

- Un accès au système et gain de privilèges

Phases d'une attaque typique

Définition du but de l'attaque

L'établissement visé

Pour une attaque structuré, l'établissement visé est choisi bien auparavant. Par exemple:

- Un concurrent
- Un "convive" (au réseau LAN)
- L'ex-société
- Un site e-commercial

Objectifs

- Un accès au système et gain de privilèges
- Un déni de service

Phases d'une attaque typique

Reconnaissance avant l'attaque

Objectif

Collecter le maximum d'informations à propos de la cible

Exemples d'informations

Phases d'une attaque typique

Reconnaissance avant l'attaque

Objectif

Collecter le maximum d'informations à propos de la cible

Exemples d'informations

- Les adresses IP des machines

Phases d'une attaque typique

Reconnaissance avant l'attaque

Objectif

Collecter le maximum d'informations à propos de la cible

Exemples d'informations

- Les adresses IP des machines
- La topologie réseau et localisation des dispositifs de contrôle d'accès

Phases d'une attaque typique
Reconnaissance avant l'attaque

Objectif

Collecter le maximum d'informations à propos de la cible

Exemples d'informations

- Les adresses IP des machines
- La topologie réseau et localisation des dispositifs de contrôle d'accès
- Ports ouverts

Phases d'une attaque typique

Reconnaissance avant l'attaque

Objectif

Collecter le maximum d'informations à propos de la cible

Exemples d'informations

- Les adresses IP des machines
- La topologie réseau et localisation des dispositifs de contrôle d'accès
- Ports ouverts
- Protocoles réseau et OS

Phases d'une attaque typique

Reconnaissance avant l'attaque

Objectif

Collecter le maximum d'informations à propos de la cible

Exemples d'informations

- Les adresses IP des machines
- La topologie réseau et localisation des dispositifs de contrôle d'accès
- Ports ouverts
- Protocoles réseau et OS
- Les adresses e-mail du personnel

Phases d'une attaque typique

Choix et lancement de l'attaque

Gain d'accès

On choisit l'équipement (serveur, routeur ...) le plus vulnérable à une attaque. Puis, on lance un écoute du trafic ou cheval de Troie

Déni de service

- On choisit un équipement cruciale au bon fonctionnement du système cible
- Après, on choisit la technique qui causera un déni de service

Phases d'une attaque typique

Après l'attaques

Gain d'accès réussi

Un DOS réussi

Phases d'une attaque typique
Après l'attaques

Gain d'accès réussi

- On essaye d'augmenter nos privilège

Un DOS réussi

Phases d'une attaque typique

Après l'attaques

Gain d'accès réussi

- On essaye d'augmenter nos privilège
- On cherche à causer plus de dégâts

Un DOS réussi

Phases d'une attaque typique

Après l'attaques

Gain d'accès réussi

- On essaye d'augmenter nos privilège
- On cherche à causer plus de dégâts
- On établit des "backdoor" pour des connexions plus flexibles

Un DOS réussi

Phases d'une attaque typique
Après l'attaques

Gain d'accès réussi

- On essaye d'augmenter nos privilège
- On cherche à causer plus de dégâts
- On établit des "backdoor" pour des connexions plus flexibles
- On cherche à supprimer nos traces

Un DOS réussi

Phases d'une attaque typique

Après l'attaques

Gain d'accès réussi

- On essaye d'augmenter nos privilège
- On cherche à causer plus de dégâts
- On établit des "backdoor" pour des connexions plus flexibles
- On cherche à supprimer nos traces

Un DOS réussi

- Diffuser la nouvelle

Plan

Menaces liées à la couche liaison de données



Menaces liées à la couche liaison de données

- **MAC Flooding**:
- **MAC Spoofing**:
- **ARP Cache poisoning**
- **DHCP Spoofing**:

Menaces liées à la couche liaison de données

- **MAC Flooding**: Cette attaque consiste à submerger une interface du *commutateur* par de nombreuses adresses MAC. Selon le commutateur, il se peut qu'il y est une panne ou bien il commence à agir comme un *concentrateur*
- **MAC Spoofing**:
- **ARP Cache poisoning**
- **DHCP Spoofing**:

Menaces liées à la couche liaison de données

- **MAC Flooding**: Cette attaque consiste à submerger une interface du *commutateur* par de nombreuses adresses MAC. Selon le commutateur, il se peut qu'il y est une panne ou bien il commence à agir comme un *concentrateur*
- **MAC Spoofing**: Modifier son adresse MAC en une autre qui existe dans le même réseau en vu d'intercepter son flux entrant
- **ARP Cache poisoning**
- **DHCP Spoofing**:

Menaces liées à la couche liaison de données

- **MAC Flooding**: Cette attaque consiste à submerger une interface du *commutateur* par de nombreuses adresses MAC. Selon le commutateur, il se peut qu'il y est une panne ou bien il commence à agir comme un *concentrateur*
- **MAC Spoofing**: Modifier son adresse MAC en une autre qui existe dans le même réseau en vu d'intercepter son flux entrant
- **ARP Cache poisoning**
- **DHCP Spoofing**: Introduire un serveur DHCP

Menaces liées à la couche réseau



Menaces liées à la couche réseau

- **IP Spoofing**:
- **Ping of death**:
- **Source routing**:
- **Smurf attack**:

Menaces liées à la couche réseau

- **IP Spoofing**: Cela consiste à envoyer des paquets avec une adresse IP source falsifiée
- **Ping of death**:
- **Source routing**:
- **Smurf attack**:

Menaces liées à la couche réseau

- **IP Spoofing**: Cela consiste à envoyer des paquets avec une adresse IP source falsifiée
- **Ping of death**: Cela consiste à envoyer un énorme et mal formé "ping" en vu de faire crasher la cible
- **Source routing**:
- **Smurf attack**:

Menaces liées à la couche réseau

- **IP Spoofing**: Cela consiste à envoyer des paquets avec une adresse IP source falsifiée
- **Ping of death**: Cela consiste à envoyer un énorme et mal formé "ping" en vu de faire crasher la cible
- **Source routing**: Cela permet de spécifier la route que doit prendre un paquet
- **Smurf attack**:

Menaces liées à la couche réseau

- **IP Spoofing**: Cela consiste à envoyer des paquets avec une adresse IP source falsifiée
- **Ping of death**: Cela consiste à envoyer un énorme et mal formé "ping" en vu de faire crasher la cible
- **Source routing**: Cela permet de spécifier la route que doit prendre un paquet
- **Smurf attack**: Cela consiste à envoyer un ping à une adresse broadcast tout en modifiant l'IP source de ce ping. Résultat: La machine usurpé va être submergée de réponse ICMP

Menaces liées à la couche transport

Menaces liées à la couche transport

- **SYN Flooding**:
- **UDP Flooding**:

Menaces liées à la couche transport

- **SYN Flooding**: On essaye de multiplier les demandes de connexions TCP sans jamais les confirmer.
- **UDP Flooding**:

Menaces liées à la couche transport

- **SYN Flooding**: On essaye de multiplier les demandes de connexions TCP sans jamais les confirmer.
- **UDP Flooding**: On essaye de générer un grand nombre de datagramme dans un réseau cible.

Plan

Noeuds réseau

Noeuds réseau

- **Concentrateur (hub)**

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**
- **Routeur (router)**

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**
- **Routeur (router)**
- **Parfeu (firewall)**

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**
- **Routeur (router)**
- **Parfeu (firewall)**
    - Parfeu sans état
    - Parfeu à états
    - Parfeu applicatif

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**
- **Routeur (router)**
- **Parfeu (firewall)**
  - Parfeu sans état
  - Parfeu à états
  - Parfeu applicatif
- **Proxy**

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**
- **Routeur (router)**
- **Parfeu (firewall)**
  - Parfeu sans état
  - Parfeu à états
  - Parfeu applicatif
- **Proxy**
  - Proxy d'authentification
  - Proxy d'anonymat
  - Proxy de mise en cache
  - Proxy de filtrage

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**
- **Routeur (router)**
- **Parfeu (firewall)**
  - Parfeu sans état
  - Parfeu à états
  - Parfeu applicatif
- **Proxy**
  - Proxy d'authentification
  - Proxy d'anonymat
  - Proxy de mise en cache
  - Proxy de filtrage
- **NIDS/NIPS**

Noeuds réseau

- **Concentrateur (hub)**
- **Commutateur (switch)**
- **Routeur (router)**
- **Parfeu (firewall)**
  - Parfeu sans état
  - Parfeu à états
  - Parfeu applicatif
- **Proxy**
  - Proxy d'authentification
  - Proxy d'anonymat
  - Proxy de mise en cache
  - Proxy de filtrage
- **NIDS/NIPS**
- **Les pots de miel**

Architecture réseaux

Agrégation de lien

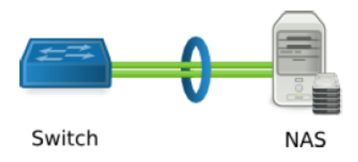


Figure : Agrégation de lien

Objectif:

Architecture réseaux

Agrégation de lien

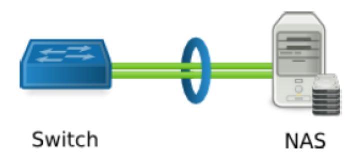


Figure : Agrégation de lien

Objectif: Augmenter la disponibilité

Architecture réseaux

La zone démilitarisée

La DMZ est une zone de l'intranet qui est exposée à un réseau extérieur non sécurisé.

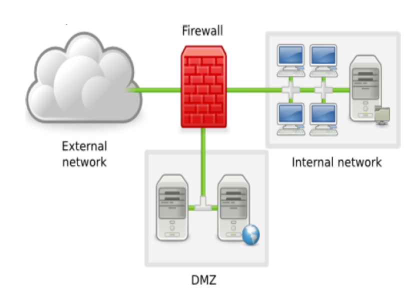


Figure : Single firewalled DMZ

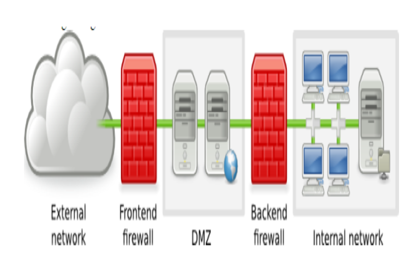


Figure : Dual firewalled DMZ

Architecture réseaux

Les Vlans - Virtual LAN

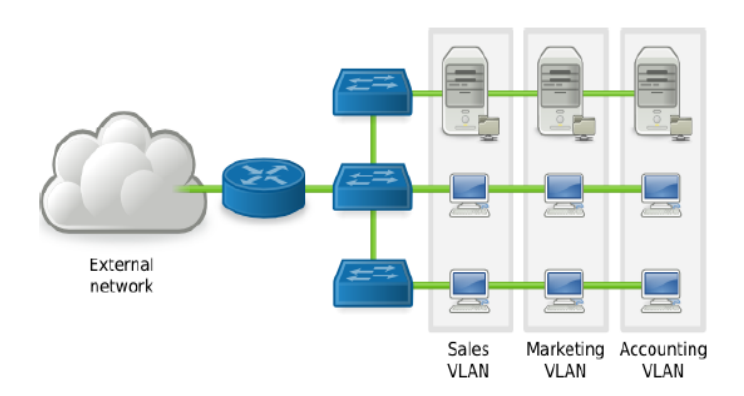


Figure : Vlan

Architecture réseaux

Les VPN - Virtual Private Network

Définition

Protocoles

Architecture réseaux

Les VPN - Virtual Private Network

Définition

- Un VPN est un réseau informatique dans lequel une communication nécessite le passage sûr depuis un réseau non sécurisé.
- Types:

Protocoles

Architecture réseaux

Les VPN - Virtual Private Network

Définition

- Un VPN est un réseau informatique dans lequel une communication nécessite le passage sûr depuis un réseau non sécurisé.
- Types:
  - Site to site VPN
  - Remote acces VPN

Protocoles

Architecture réseaux

Les VPN - Virtual Private Network

Définition

- Un VPN est un réseau informatique dans lequel une communication nécessite le passage sûr depuis un réseau non sécurisé.
- Types:
  - Site to site VPN
  - Remote acces VPN

Protocoles

Pour assurer la sécurité du flux expédié dans le réseau non sûre, les VPN font recours à des protocoles de tunneling:

- PPTP - Point-To-Point Tunneling Protocol
- GRE - Generic Routing Encapsulation
- L2TP - Layer 2 Tunneling Protocol
- IPsec - Internet Protocol Security

IPsec - IP Security Protocols

Définition

Caractéristiques

IPsec - IP Security Protocols

Définition

L'IPsec est un ensemble de protocoles qui ont pour vocation la sécurisation des communications au niveau 3 du modèle OSI

Caractéristiques

IPsec - IP Security Protocols

Définition

L'IPsec est un ensemble de protocoles qui ont pour vocation la sécurisation des communications au niveau 3 du modèle OSI

Caractéristiques

- Il est nativement compatible avec l'IPv6

IPsec - IP Security Protocols

Définition

L'IPsec est un ensemble de protocoles qui ont pour vocation la sécurisation des communications au niveau 3 du modèle OSI

Caractéristiques

- Il est nativement compatible avec l'IPv6
- Il peut être utilisé sous deux modes différents: transport ou tunnel

IPsec - IP Security Protocols

Définition

L'IPsec est un ensemble de protocoles qui ont pour vocation la sécurisation des communications au niveau 3 du modèle OSI

Caractéristiques

- Il est nativement compatible avec l'IPv6
- Il peut être utilisé sous deux modes différents: transport ou tunnel
- La SA (Security associations) définit les protocoles et les paramètres que deux entités peuvent utiliser pour l'établissement d'une communication IPsec

IPsec - IP Security Protocols

Définition

L'IPsec est un ensemble de protocoles qui ont pour vocation la sécurisation des communications au niveau 3 du modèle OSI

Caractéristiques

- Il est nativement compatible avec l'IPv6
- Il peut être utilisé sous deux modes différents: transport ou tunnel
- La SA (Security associations) définit les protocoles et les paramètres que deux entités peuvent utiliser pour l'établissement d'une communication IPsec
- Chaque entrée dans la base de donnée des SA est identifiée par un indice SPI (Security Parameters Index)

IPsec - IP Security Protocols

Protocoles IPsec

L'IPsec repose sur l'utilisation des protocoles suivants:

IPsec - IP Security Protocols

Protocoles IPsec

L'IPsec repose sur l'utilisation des protocoles suivants:

- AH (Authentification Header): Pour assurer l'authenticité et l'intégrité des datagrammes IP

IPsec - IP Security Protocols

Protocoles IPsec

L'IPsec repose sur l'utilisation des protocoles suivants:

- AH (Authentification Header): Pour assurer l'authenticité et l'intégrité des datagrammes IP
- ESP (Encapsulating Security Payload): Pour assurer la confidentialité des données et l'authenticité des datagrammes IP

IPsec - IP Security Protocols

Protocoles IPsec

L'IPsec repose sur l'utilisation des protocoles suivants:

- AH (Authentification Header): Pour assurer l'authenticité et l'intégrité des datagrammes IP
- ESP (Encapsulating Security Payload): Pour assurer la confidentialité des données et l'authenticité des datagrammes IP
- Ces deux protocoles sont souvent utilisés conjointement

IPsec - IP Security Protocols

Protocoles IPsec

L'IPsec repose sur l'utilisation des protocoles suivants:

- AH (Authentification Header): Pour assurer l'authenticité et l'intégrité des datagrammes IP
- ESP (Encapsulating Security Payload): Pour assurer la confidentialité des données et l'authenticité des datagrammes IP
- Ces deux protocoles sont souvent utilisés conjointement
- Le protocole IKE se charge de la gestion des paramètres des protocoles utilisés

Composantes IPsec

Composantes IPsec

Composantes IPsec

Composantes IPsec

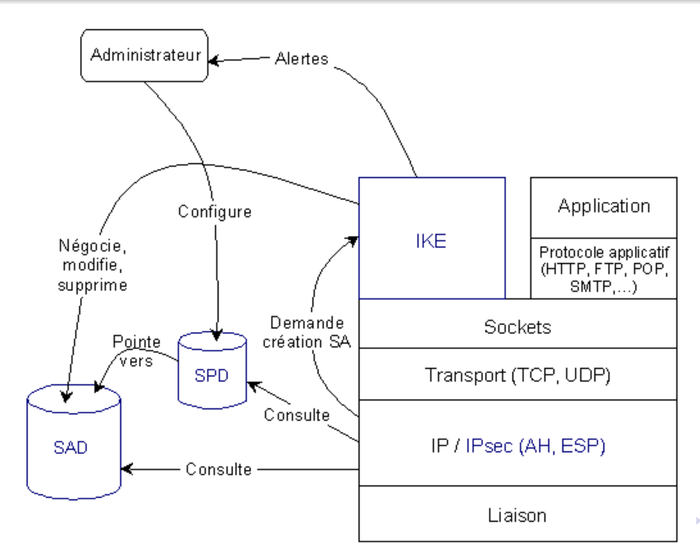
- SAD - Security Association Database: ce composant fait l'inventaire de toutes les SA actives dans un système

Composantes IPsec

Composantes IPsec

- SAD - Security Association Database: ce composant fait l'inventaire de toutes les SA actives dans un système
- SPD - Security Policy Database): ce composant détermine les règles de sécurité à appliquer sur chaque paquet selon la SA

Principe de fonctionnement de l'IPsec



Principe de fonctionnement de l'IPsec

Scénarios

Trafic entrant

- Paquet reçu
- Examen de l'entête pour voir s'il a subit un service (ou plusieurs) IPsec
- Si oui, on y cherche les références de la SA qui a été utilisée. Sinon, la SPD[a] décide s'il a le droit de passer (des paquets IKE)
- Consultation de la SAD[b] pour utiliser les paramètres de cette SA (Authentification et/ou déchiffrement)

---

[a]Security Policy Database
[b]Security Association Database

Principe de fonctionnement de l'IPsec
Scénarios

Trafic sortant

- Paquet à envoyer
- Consultation de la SPD pour savoir si le paquet doit être traité par les mécanismes IPsec
- Si c'est le cas, on consulte la SAD pour savoir quel SA sera appliqué au paquet
- Si la SA n'existe pas encore, l'IKE se charge d'en créer une nouvelle

Protocoles de l'IPsec

AH - Authentication Header

Protocoles de l'IPsec

AH - Authentication Header

Le protocole AH ajoute simplement une entête au paquet qu'on veut sécuriser. Il est utilisé pour assurer:

Protocoles de l'IPsec

AH - Authentication Header

Le protocole AH ajoute simplement une entête au paquet qu'on veut sécuriser. Il est utilisé pour assurer:

- L'authentification
- L'intégrité
- L'anti-rejeu

Protocoles de l'IPsec

ESP - Encapsulating Security Payload

Protocoles de l'IPsec

ESP - Encapsulating Security Payload

Le protocole ESP prend le paquet à sécuriser et chiffre ses données et optionnellement son entête. Il encapsule le paquet résultant avec une entête et une queue et optionnellement une autre queue pour des besoins d'authentification. Il est utilisé pour assurer:

Protocoles de l'IPsec

ESP - Encapsulating Security Payload

Le protocole ESP prend le paquet à sécuriser et chiffre ses données et optionnellement son entête. Il encapsule le paquet résultant avec une entête et une queue et optionnellement une autre queue pour des besoins d'authentification. Il est utilisé pour assurer:

- La confidentialité au premier degré
- L'authentification
- L'anti-rejeu
- L'intégrité

L'IKE - Internet Key Exchange

Rôle

L'IKE - Internet Key Exchange

Rôle

Ce protocole est le responsable de l'échange des clés de chiffrement et de déchiffrement de manière sécurisée. Il se manifeste en deux étapes:

L'IKE - Internet Key Exchange

Rôle

Ce protocole est le responsable de l'échange des clés de chiffrement et de déchiffrement de manière sécurisée. Il se manifeste en deux étapes:

1. Création d'un tunnel administratif où se passera la négociation des protocoles d'authentification et de chiffrement

L'IKE - Internet Key Exchange

Rôle

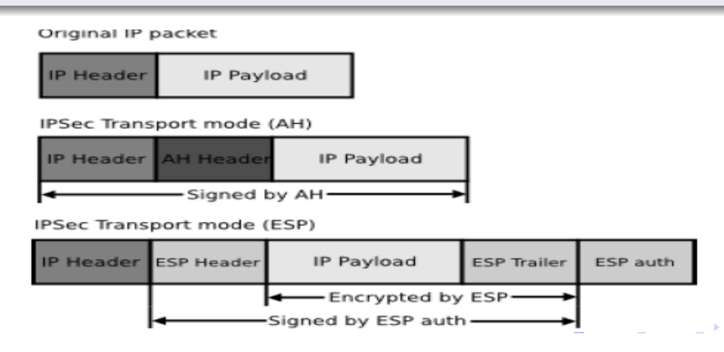
Ce protocole est le responsable de l'échange des clés de chiffrement et de déchiffrement de manière sécurisée. Il se manifeste en deux étapes:

1. Création d'un tunnel administratif où se passera la négociation des protocoles d'authentification et de chiffrement
2. Création d'un deuxième tunnel pour l'échange de données

Les modes de l'IPsec

Mode transport

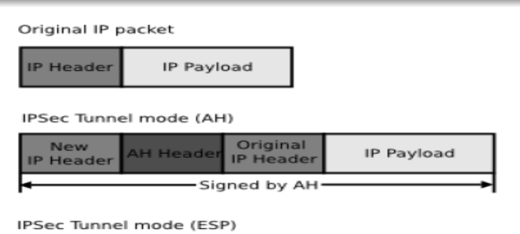
Ce mode est utilisé pour la sécurisation des communications host to host. On y utilise l'AH et/ou l'ESP. Dans ce mode, le paquet original est légèrement modifié, son champs de donnée est soit devancé par une entête AH ou bien encapsulé par l'ESP



Les modes de l'IPsec

Mode tunnel

Ce mode est utilisé pour la sécurisation des communications site to site. On y utilise l'AH et/ou l'ESP (souvent seul l'ESP est utilisé ici). Dans ce mode, le paquet original est lourdement modifié, tout le paquet est encapsulé par l'ESP



La SA de l'IPsec

Rôle

Caractéristiques

La SA de l'IPsec

Rôle

La SA définit les protocoles, les paramètres et les clés à utiliser pour sécuriser une communication donnée.

Caractéristiques

La SA de l'IPsec

Rôle

La SA définit les protocoles, les paramètres et les clés à utiliser pour sécuriser une communication donnée.

Caractéristiques

- Une SA est unidirectionnelle (donc nécessité de deux SAs sur les deux bouts d'une communication sécurisée)

La SA de l'IPsec

Rôle

La SA définit les protocoles, les paramètres et les clés à utiliser pour sécuriser une communication donnée.

Caractéristiques

- Une SA est unidirectionnelle (donc nécessité de deux SAs sur les deux bouts d'une communication sécurisée)
- Chaque SA doit contenir les identités des deux bouts de communication:

La SA de l'IPsec

Rôle

La SA définit les protocoles, les paramètres et les clés à utiliser pour sécuriser une communication donnée.

Caractéristiques

- Une SA est unidirectionnelle (donc nécessité de deux SAs sur les deux bouts d'une communication sécurisée)
- Chaque SA doit contenir les identités des deux bouts de communication:
    - Source IP et source Port
    - Destination IP et destination Port
    - Le protocole de transport (TCP/UDP)
    - Le mode et les protocoles utilisés

Plan

Plan

Administration réseau

Définition

Principes globales

Administration réseau

Définition

L'administration réseau réside en un contrôle centralisé des états de différents équipements connectés au réseau

Principes globales

Administration réseau

Définition

L'administration réseau réside en un contrôle centralisé des états de différents équipements connectés au réseau

Principes globales

- La détection des défaillances
- Le contrôle de l'utilisation de chaque équipement
- La gestion de la sécurité
- L'optimisation de l'utilisation du réseau

SNMP - Simple Network Management Protocol

[a] Management Information Base

SNMP - Simple Network Management Protocol

Le SNMP est un protocole client/serveur qui permet d'administrer les équipements du réseau. Un réseau géré par le SNMP consiste en ces trois composants:

[a] Management Information Base

SNMP - Simple Network Management Protocol

Le SNMP est un protocole client/serveur qui permet d'administrer les équipements du réseau. Un réseau géré par le SNMP consiste en ces trois composants:

- **Les équipements gérés**:
- **Les agents SNMP**:
- **Le système de management du réseau**:

[a]Management Information Base

SNMP - Simple Network Management Protocol

Le SNMP est un protocole client/serveur qui permet d'administrer les équipements du réseau. Un réseau géré par le SNMP consiste en ces trois composants:

- **Les équipements gérés**: Tout équipement qu'on souhaite administrer
- **Les agents SNMP**:
- **Le système de management du réseau**:

[a] Management Information Base

SNMP - Simple Network Management Protocol

Le SNMP est un protocole client/serveur qui permet d'administrer les équipements du réseau. Un réseau géré par le SNMP consiste en ces trois composants:

- **Les équipements gérés**: Tout équipement qu'on souhaite administrer
- **Les agents SNMP**: Un agent SNMP est un logiciel installé sur un équipement du réseau. Il a une connaissance locale de l'équipement auquel il est attaché (depuis la MIB[a]) et il est capable d'envoyer des alertes au NMS.
- **Le système de management du réseau**:

[a] Management Information Base

SNMP - Simple Network Management Protocol

Le SNMP est un protocole client/serveur qui permet d'administrer les équipements du réseau. Un réseau géré par le SNMP consiste en ces trois composants:

- **Les équipements gérés**: Tout équipement qu'on souhaite administrer
- **Les agents SNMP**: Un agent SNMP est un logiciel installé sur un équipement du réseau. Il a une connaissance locale de l'équipement auquel il est attaché (depuis la MIB[a]) et il est capable d'envoyer des alertes au NMS.
- **Le système de management du réseau**: Le point centrale depuis lequel on gère les équipements. Il agit comme un client envers ses agents

[a] Management Information Base

SNMP - Simple Network Management Protocol

Les commandes SNMP

Les commandes SNMP représentent la communication qui peut être établie entre la NMS et ses agents. Les requêtes sont envoyées sur UDP/161 vers les agents. Les réponses sont reçues sur UDP/162 vers la NMS

SNMP - Simple Network Management Protocol

Les commandes SNMP

Les commandes SNMP représentent la communication qui peut être établie entre la NMS et ses agents. Les requêtes sont envoyées sur UDP/161 vers les agents. Les réponses sont reçues sur UDP/162 vers la NMS

- **Get-request**:
- **Get-next-reuest**:
- **Set-request**:
- **Get-reponse**:
- **Trap**:

SNMP - Simple Network Management Protocol

Les commandes SNMP

Les commandes SNMP représentent la communication qui peut être établie entre la NMS et ses agents. Les requêtes sont envoyées sur UDP/161 vers les agents. Les réponses sont reçues sur UDP/162 vers la NMS

- **Get-request**: La NMS demande une information auprès de l'agent SNMP
- **Get-next-reuest**:
- **Set-request**:
- **Get-reponse**:
- **Trap**:

SNMP - Simple Network Management Protocol

Les commandes SNMP

Les commandes SNMP représentent la communication qui peut être établie entre la NMS et ses agents. Les requêtes sont envoyées sur UDP/161 vers les agents. Les réponses sont reçues sur UDP/162 vers la NMS

- **Get-request**: La NMS demande une information auprès de l'agent SNMP
- **Get-next-reuest**: La NMS demande l'information suivante auprès de l'agent SNMP
- **Set-request**:
- **Get-reponse**:
- **Trap**:

SNMP - Simple Network Management Protocol

Les commandes SNMP

Les commandes SNMP représentent la communication qui peut être établie entre la NMS et ses agents. Les requêtes sont envoyées sur UDP/161 vers les agents. Les réponses sont reçues sur UDP/162 vers la NMS

- **Get-request**: La NMS demande une information auprès de l'agent SNMP
- **Get-next-reuest**: La NMS demande l'information suivante auprès de l'agent SNMP
- **Set-request**: La NMS met à jour une information au sein d'une MIB d'un équipement
- **Get-reponse**:
- **Trap**:

SNMP - Simple Network Management Protocol

Les commandes SNMP

Les commandes SNMP représentent la communication qui peut être établie entre la NMS et ses agents. Les requêtes sont envoyées sur UDP/161 vers les agents. Les réponses sont reçues sur UDP/162 vers la NMS

- **Get-request**: La NMS demande une information auprès de l'agent SNMP
- **Get-next-reuest**: La NMS demande l'information suivante auprès de l'agent SNMP
- **Set-request**: La NMS met à jour une information au sein d'une MIB d'un équipement
- **Get-reponse**: L'agent SNMP répond à une requête de la NMS
- **Trap**:

SNMP - Simple Network Management Protocol

Les commandes SNMP

Les commandes SNMP représentent la communication qui peut être établie entre la NMS et ses agents. Les requêtes sont envoyées sur UDP/161 vers les agents. Les réponses sont reçues sur UDP/162 vers la NMS

- **Get-request**: La NMS demande une information auprès de l'agent SNMP
- **Get-next-reuest**: La NMS demande l'information suivante auprès de l'agent SNMP
- **Set-request**: La NMS met à jour une information au sein d'une MIB d'un équipement
- **Get-reponse**: L'agent SNMP répond à une requête de la NMS
- **Trap**: L'agent SNMP envoie une alerte à la NMS

SNMP - Simple Network Management Protocol

La sécurité du SNMP

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

- **SNMPv1**:
- **SNMPv2**:
- **SNMPv3**:

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

- **SNMPv1**: Aucune notion de sécurité
- **SNMPv2**:
- **SNMPv3**:

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

- **SNMPv1**: Aucune notion de sécurité
- **SNMPv2**: Problème de rétrocompatibilité
- **SNMPv3**:

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

- **SNMPv1**: Aucune notion de sécurité
- **SNMPv2**: Problème de rétrocompatibilité
- **SNMPv3**:
  - La rétrocompatibilité n'est plus un problème

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

- **SNMPv1**: Aucune notion de sécurité
- **SNMPv2**: Problème de rétrocompatibilité
- **SNMPv3**:
  - La rétrocompatibilité n'est plus un problème
  - Le contrôle d'intégrité est assuré avec les fonctions de hachages telles: MD5 et SHA-1

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

- **SNMPv1**: Aucune notion de sécurité
- **SNMPv2**: Problème de rétrocompatibilité
- **SNMPv3**:
  - La rétrocompatibilité n'est plus un problème
  - Le contrôle d'intégrité est assuré avec les fonctions de hachages telles: MD5 et SHA-1
  - La confidentialité est assurée avec le DES

SNMP - Simple Network Management Protocol

La sécurité du SNMP

La sécurité de la communication entre les composants SNMP dépend de la version utilisée du protocole

- **SNMPv1**: Aucune notion de sécurité
- **SNMPv2**: Problème de rétrocompatibilité
- **SNMPv3**:
  - La rétrocompatibilité n'est plus un problème
  - Le contrôle d'intégrité est assuré avec les fonctions de hachages telles: MD5 et SHA-1
  - La confidentialité est assurée avec le DES
  - L'anti-rejeu est assuré avec un mécanisme d'estampillage

Outils d'administrations

- Nagios
- Zabbix
- Cacti
- Munin
- MRTG
- ...

Plan

Réseau WIFI

Définition

Un réseau wifi est un réseau local sans fil qui utilise les ondes radio comme média de transport.

Conséquence

Utiliser les ondes radio comme média de transport implique la diffusion des données de tout part en l'air.

Réaction

Plusieurs mécanismes de sécurisation ont vu jour. On en cite:

- WEP (Wired Equivalent Privacy)
- WPA/WPA2 (WiFi Protected Access)

WEP (Wired Equivalent Privacy)

Le WEP

Le WEP a été désigné au 1999. Il a pour objectif d'assurer la confidentialité des communications

Caractéristiques

- L'algorithme RC4 pour le chiffrement des données
- L'algorithme CRC32 pour la vérification de l'intégrité des trames
- 40 ou 140 bits comme taille des clés
- 24 bits pour le vecteur d'initialisation
- 64 ou 128 bits comme taille de clé pour le RC4

WEP (Wired Equivalent Privacy)

Le WEP

Ce mécanisme est devenu obsolète. Depuis 2001, plusieurs articles ont vu le jour qui démontrent sa faiblesse. En 2006, on arrive à cracker la clé WEP en quelque secondes grâce à la fragmentation des paquets[a]. De plus, la clé est partagé par tous les noeuds.

[a] A. Bittau, M. Handley and J. Lackey *The Final Nail in WEP's Coffin*

Solution

- Mise en place du VPN (si l'utilisation du WEP n'est pas un choix)
- Passer aux WPA et WPA2

WPA/WPA2 (WiFi Protected Access)

Le WPA

Le WPA est aussi un mécanisme de sécurisation des réseaux wifi. Les travaux sur ce mécanisme ont vu le jour en 2003 dans le but d'améliorer le WEP.

Caractéristiques

- Le même algorithme de chiffrement (RC4, pour garder une compatibilité avec le WEP). Mais, implémenté dans une façon différente
- Le MIC pour l'intégrité des trames (plus robuste que le CRC32)
- 48 bits pour la taille du vecteur d'initialisation

WPA/WPA2 (WiFi Protected Access)

Le WPA2

Le WPA2 est le successeur du WPA. Il est certifié par la *Wi-Fi Alliance* et se base sur le mécanisme CCMP[a] (Le CCMP est considéré comme complètement sécurisé)

[a] CBC-MAC Counter Mode Protocol

Caractéristiques

- AES au lieu du RC4
- Clé temporaire de 128 bits
- WPA personnelle: basé sur le PSK (PreShared key)
- WPA entreprise: basé sur 802.1x (ex: Radius)